

MS-200 Network Masking Capabilities

About Masking Networks

Masking Networks is based in Reston, Virginia. Our primary customer has been the U.S. Department of Defense (DOD) and we are expanding our business in Homeland Security and Energy. Our primary point of contact is the CEO, John Nelson, by email to jnelson@maskingnetworks.com.

Summary

Cyber attackers have the advantage today because networks are static or slow to change and the attacker can lie in wait, gather intelligence, and attack on their own terms. Masking Networks' approach is to make networks more dynamic by masking key identifying information in network packets while retaining compatibility and performance. This is consistent with the new National Cyber Security Policy calling for breakthrough "Moving Targets" network defenses.

The MS-200 product line is at Technology Readiness Level (TRL) 5/6. Our first generation MS-100SC is TRL 8/9, is in production, and has been vetted by DOD. **Primary use cases include masking a multiport firewall and masking end nodes in a mesh switch network.** This provides more effective network segmentation and prevents traffic analysis, ARP spoofing, and other layer 2 / 3 attacks.

The Value of Network Masking

Network protocols are implemented in logical layers. The network addresses of a device are its Layer 2 "MAC" address and Layer 3 "IP" address. Cyber attackers rely on the static relationship between a device and these addresses to plan and carry out their attacks.

One way to address this vulnerability is to make these static network addresses dynamic thus causing the cyber attackers' probing to yield useless or misleading results. The attackers must then choose to give up or attack more "noisily" and risk being detected and countered by the defender.

This is validated by real-world experience. For example, "Red Hat" security auditors also exploit these static relationships for penetration testing.

And, Firewall, switch and intrusion detection (IDS) manufacturers consistently warn customers about the threats at Layer 2 and Layer 3 because their products keep track of these static relationships and therefore are often prime targets of cyber attacks.

MS-200 Theory of Operation

The MS-200 operates as a masking switch and dynamically masks the network addresses of all devices directly connected to its ports. For example, the MAC addresses are randomly generated, can be regenerated within very short intervals, and are resolved cryptographically. The MS 200 also supports loadable software modules, event logging, and inter-device communication.

Wire speed performance is achieved by modifying specific portions of network packets using digital signal processing techniques. The network masking device itself requires no MAC address and is completely invisible to the cyber attacker. This effectively blinds the cyber attacker by masking the identity and presence of firewalls, servers, virtual machine managers, LAN segments, IDS and other critical devices while maintaining full network compatibility and performance.

We are also seeking strategic partners to prototype the integration of the MS-200 network masking circuit in a 3rd party switch to more broadly address enterprise networks.

Network masking offers clear value as a passive due-care network defense. And, teamed with other security devices, it also enhances attack detection and response. For example, network masking forces the attacker to use more active techniques that can be easily identified by intrusion detection and prevention systems (IDS / IPS). A network masking device could also coordinate with other masking devices to modify network packets in such a way as to lure, repel, or isolate an attacker.

Uniqueness of Approach

The MS-100SC is protected by United States Patent 7712130, issued May 4, 2010 as well as patents in other countries. All patents are fully assigned to Masking Networks. We expect to file additional patents with the MS-200.

MS 200 & Network Security

Network Defense	<ul style="list-style-type: none"> • Generate dynamic MAC and IP address proxies and mask network hops <ul style="list-style-type: none"> ○ Prevent network mapping ○ Prevent traffic analysis ○ Confuse zero-day attacks • Render firewalls, IDS and other hosts transparent to attacker while retaining full function to route traffic and communicate • Host a firewall or be integrated in 3rd party firewall
Threat Detection	<ul style="list-style-type: none"> • Force intruder to give up or use more active techniques which trigger IDS / IPS detection • Work in conjunction with other MS 200s or IPS to detect threats • Host an IDS or be integrated in 3rd party IDS
Offensive Response	<ul style="list-style-type: none"> • Automatically defeat internal MAC or IP man-in-the-middle attack • Delay attacker with dynamic and deceptive results • Work in conjunction with other MS 200 circuits to lure or isolate attacker • Host dynamic firewall or IPS

Competitive Approaches

Transparent Firewalls and IDS: Most firewalls and IDS have an optional mode in which they do not broadcast their MAC address. This mode hides the firewall or IDS but significantly limits its functionality as it cannot route traffic or communicate with other devices.

Switch Port Security: Many switches have a “port security” mode where a port is configured to only allow connection by a pre-configured set of device MAC addresses. This approach imposes a significant configuration management burden and actually makes the network even more static,

running counter to the basic premise of “Moving Targets” defense.

MAC Address Masking: Software is available for personal computers and other hosts to substitute a static proxy MAC address for the MAC address burned into their network card at manufacturing. This approach may delay the cyber attacker in identifying the device type and its capabilities. However, this is also a static technique and so does not protect the device from eventual mapping, MAC spoofing or other low level attacks.

Network Address Translation (NAT): Routers and gateways may be configured to translate IP addresses for the devices they route traffic for. This is a common technique for getting around the overall limit on IP address space in IPv4. As such this is not implemented in a way that is intended to provide dynamic security and even the NAT device itself is vulnerable to attack.

Summary: Masking Networks’ approach provides a stronger “moving targets” defense without increasing the network management burden and while maintaining full network performance and compatibility.

Customer Validation

The MS-100SC won honors at CWID 2005 and was funded for evaluation and operational tests from 2006 – 2009 at JFCOM, SPAWAR and DISA. In all tests the MS-100SC performed to specification and the evaluation also yielded expanded functional requirements that have been incorporated into the feature set of the MS-200 product line. This includes the feasibility for integrating the MS-200 technology in a 3rd party network switch.

Company Information

Organization: Delaware C-Corp

HQ Location: Reston, Virginia

All products sourced and manufactured in the U.S.

DUNS: 793473716

CAGE: 4TGW2

SBA: Small Business

NAICS: 334210, 334220

PSC: 5810, 5865